FONDATION UNIVERSITE SAVOIE MONT BLANC

27 rue Marcoz, 73000 Chambéry
dir.fondation@univ-smb.fr

Lundi 6 juillet 2020

Covid-19 : application mobiles & protection de la vie privée

***Motahareh Fathisalout Bollon**, enseignante-chercheure à la Faculté de droit*

Durant cette période de crise, nos propos de chercheurs “Soigner des maux avec des mots” ont tenté d’apporter un éclairage sur une situation donnée. Il est maintenant temps de nous tourner vers notre avenir pour tenter de le rendre meilleur et plus sûr ! Tel est l’objet de cette chronique.

Aujourd’hui Motahareh Fathisalout Bollon, enseignante-chercheure à la Faculté de droit, revient sur la règlementation des applications mobiles numériques, avec, en toile de fond StopCovid.

La période de confinement avait été propice au téléchargement d’applications en tous genres (y compris pour se déplacer). Plus récemment StopCovid, l’application qui s’inscrit dans le plan global de déconfinement du Gouvernement, a fait couler pas mal d’encre. Vous qui travaillez sur la règlementation des applications mobiles numériques, quels sont les risques ?

Il faut d’abord souligner le contexte de l’apparition de cette application. Alors que la pandémie de Covid-19 faisait rage dans le monde entier, la principale mesure d’atténuation a été la distanciation sociale extrême et les mesures de confinement obligatoires, appuyées par des Ordonnances, dans de nombreux pays. Pris entre l’effondrement économique et la catastrophe sociale, de nombreux gouvernements ont adopté des décrets d’urgence et multiplié les mesures qui peuvent porter atteinte aux libertés civiles et aux droits fondamentaux.

Pour limiter la propagation, un prolongement de la durée des mesures de distanciation sociale extrême semblait nécessaire, sauf à mobiliser la technologie pour cibler les personnes atteintes et appliquer une mise en quarantaine ciblée. C’est ainsi qu’un consensus s’est formé autour d’une stratégie combinant les ressources médicales et les outils technologiques pour fournir une réponse à une échelle susceptible de prendre en vitesse la propagation du virus. Certains pays ont progressivement mis en place des applications mobiles (p. ex. : NHS Covid-19 au Royaume-Uni, CovidRadar au

DECOUVREZ TOUS LES « PROPOS DE CHERCHEURS » SUR : www.fondation-usmb.fr/propos-de-chercheurs

Mexique, CovidSafe en Australie, Mask.ir en Iran, etc. [1]), qui sont plus ou moins intrusives et dont le fonctionnement nécessite la collecte, en temps réel, de données, à caractère personnel, voire sensible. Ainsi, le système chinois, appelé « Chinese health code system », récolte des données telles que l'identité des citoyens, leur localisation et même l'historique des paiements en ligne, afin que la police locale puisse surveiller ceux qui enfreignent les règles de quarantaine. En fonction de la technologie employée (p. ex. : Bluetooth, GPS, API, DP-3T), les applications peuvent être plus ou moins intrusives. Les interrogations se sont multipliées : quelles sont les données collectées et avec qui seront-elles partagées ? Comment ces informations seront-elles utilisées à l'avenir ? Quelles mesures ont été mises en place pour prévenir les abus ?

Sur quoi doit porter la vigilance des utilisateurs ?

S'agissant de l'application StopCovid, mise en place par le gouvernement français, une réponse peut être apportée au regard de la technologie utilisée par l'application. StopCovid mobilise la technologie Bluetooth. Elle enregistre de façon cryptée, dans l'historique de l'application, les informations relatives à ses utilisateurs, qui se croisent dans un périmètre de moins d'un mètre et pendant 15 minutes. Ce dispositif, qui repose sur le volontariat, n'est pas l'élément central de la stratégie française de lutte contre l'épidémie de Covid-19. La technologie Bluetooth, utilisée par StopCovid semble constituer la meilleure option pour une mise en œuvre stricte de la protection de la vie privée, dans la mesure où seuls les signaux communiqués entre les smartphones sont stockés sous forme de données cryptées. Ce dispositif met les données des utilisateurs à l'abri des tiers intéressés par ces données.

Ainsi, par l'application StopCovid, les autorités françaises tendent à trouver un équilibre entre la nécessaire lutte contre cette épidémie (qui relève de l'objectif à valeur constitutionnelle de protection de la santé) et les atteintes au droit à la protection de la vie privée, notamment par la collecte et le traitement de données à caractère personnel, d'une particulière sensibilité à l'échelle nationale.

Est-ce que la période est propice à faire bouger les choses en matière de règlementation ?

Sur ce point, la Commission Nationale de l'Informatique et des Libertés (CNIL), qui veille au respect de la conformité des traitements de données personnelles au RGPD et à la loi "Informatique et Libertés", a considéré que l'atteinte portée

[1] Pour un aperçu des applications par pays, voyez : P. Howell O'Neill, T. Ryan-Mosley, B. Johnson, "Covid Tracking Tracker", MIT Technology Review, publié le 7 mai 2020 et disponible en ligne gratuitement à l'adresse suivante : https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/?truid=86e73017824ada51f2218ec0bd28885a&utm_source=engagement_email&utm_medium=email&utm_campaign=site_visitor.unpaid.engagement&utm_content=05.12.non-subs

aux droits et libertés individuels a été justifiée par un motif d'intérêt général (ici, lutte contre l'épidémie). Elle a précisé que cette atteinte est également nécessaire et proportionnée à la réalisation de cet objectif. La validation du dispositif par cette autorité rend crédible l'action du gouvernement et offre un avis, que nous espérons aussi neutre que possible, sur les risques encourus par les utilisateurs. C'est cette connaissance des risques, établie par une autorité telle que la CNIL, qui permet d'apporter une réponse à ceux qui ont peur de ce type d'application ; la peur de diffusion d'informations relatives à l'état de santé et de l'historique de déplacement… ; diffusion qui pourrait donner lieu à des stigmatisations, du harcèlement ou des boycotts (pour les entreprises notamment).

Le succès du dispositif dépend de la garantie offerte aux utilisateurs. L'objectif est de lui assurer un contrôle total sur l'utilisation des données et la divulgation des informations. Il dépend aussi de la nécessité d'un choix d'utilisation éclairé de la part des citoyens, ce qui suppose une compréhension réaliste des risques de l'utilisation de l'application.

Y aura-t-il un avant et un après Covid en la matière ?

Si l'engagement des citoyens est essentiel à la réussite du dispositif, il convient de rappeler qu'aucune solution technique ne peut garantir de manière absolue le respect de la vie privée. Par exemple, d'autres applications installées sur un smartphone peuvent interférer avec StopCovid et envoyer des données à un tiers. Ce type de risque existe de façon générale, dès lors que les données collectées par les applications disponibles sur le smartphone et/ou les appareils connectés (montre, bracelet, etc.) sont mises à disposition de tiers intéressés, avec un semblant d'assentiment de l'utilisateur (qui clique quasi mécaniquement, sur « j'ai compris » ou « j'accepte » ces conditions générales d'utilisation ou de service). Le plus important, en la matière, est d'utiliser la technologie de façon consciente.